

**CLARKSON LAW FIRM, P.C.**  
Yana Hart (SBN 306499)  
[yhart@clarksonlawfirm.com](mailto:yhart@clarksonlawfirm.com)  
Mark Richards (SBN 321252)  
[mrichards@clarksonlawfirm.com](mailto:mrichards@clarksonlawfirm.com)  
Bryan P. Thompson (SBN 354683)  
[bthompson@clarksonlawfirm.com](mailto:bthompson@clarksonlawfirm.com)  
22525 Pacific Coast Highway  
Malibu, CA 90265  
Tel: (213) 788-4050

**MILBERG COLEMAN BRYSON  
PHILLIPS GROSSMAN, PLLC**  
John J. Nelson (SBN 317598)  
[jnelson@milberg.com](mailto:jnelson@milberg.com)  
280 S. Beverly Drive  
Beverly Hills, CA 92102  
Tel: (858) 209-6941

**CLAYEO C. ARNOLD  
A PROFESSIONAL CORPORATION**  
M. Anderson Berry (SBN 262879)  
[aberry@justice4you.com](mailto:aberry@justice4you.com)  
Gregory Haroutunian (SBN 330263)  
[gharoutunian@justice4you.com](mailto:gharoutunian@justice4you.com)  
12100 Wilshire Boulevard, Suite 800  
Los Angeles, CA 90025  
Tel: (747) 777-7748  
Fax: (916) 924-1829

*Interim Co-Lead Counsel for Plaintiffs and  
the Proposed Class*

**UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA**

In re SAG Health Data Breach  
Litigation

This Document Relates to: All  
Actions

Lead Case No. 2:24-cv-10503-MEMF-JPR  
CONSOLIDATED ACTION

**CONSOLIDATED CLASS ACTION  
COMPLAINT**

DEMAND FOR JURY TRIAL

1 Plaintiffs Matthew Rouillard, Kristy Munden, Lee Wilkof, Steven Barr, and  
2 Massimiliano Furlan (“Plaintiffs”) individually and on behalf of all others similarly  
3 situated, (“Plaintiffs”) bring this Action against SAG-AFTRA Health Plan (“SAG  
4 Health” or “Defendant”), and allege upon personal knowledge as to their own actions  
5 and their counsels’ investigation, and upon information and belief as to all other  
6 matters, as follows:

7 **I. INTRODUCTION**

8 1. SAG Health provides a comprehensive health care benefits program for  
9 eligible participants and their dependents in the entertainment industry. Entertainment  
10 workers can earn eligibility through employment with producers who have signed a  
11 collective bargaining agreement with the entertainment industry’s largest union: the  
12 Screen Actors Guild-American Federation of Television and Radio Artists (“**SAG-  
13 AFTRA**”). Tens of thousands of SAG-AFTRA members have availed themselves of  
14 SAG Health’s offerings, which include a wide range of medical services.

15 2. To obtain any of these services, members are required to entrust SAG  
16 Health with their highly sensitive and personally identifiable information (“**PII**”) and  
17 personal health information (“**PHI**”), which SAG Health uses to engage in its usual  
18 business activities. SAG Health understands that it has a responsibility to protect the  
19 data it collected from unauthorized access, assuring its customers that it is “committed  
20 to protecting [members’] privacy.”<sup>1</sup> Despite this assurance to its customers, however,  
21 SAG Health failed to protect the very customer information it was entrusted,  
22 compromising the personal information of an undisclosed number of its members  
23 (“**The Data Breach**”), announced by Defendant on December 2, 2024.<sup>2</sup>

24 3. SAG Health failed to properly secure and safeguard the highly valuable,

25  
26 1 SAG-AFTRA Health Plan Privacy Policy, SAG-AFTRA Health Plan (2019),  
<https://www.sagafttraplans.org/health/privacy> (last accessed July 31, 2025).

27 2 SAG-AFTRA Health Plan Email Phishing Notice, SAG-AFTRA Health Plan  
28 (2024), <https://www.sagafttraplans.org/health/emailphishingnotice> (last accessed July  
31, 2025).

1 PII and PHI of its members, including their names, Social Security numbers, and  
2 information associated with claims and health insurance information, and other  
3 sensitive medical and non-medical data (collectively, “**Private Information**”), failed  
4 to comply with industry standards to protect information systems that contain Private  
5 Information, and failed to provide timely and adequate notice to Plaintiffs and other  
6 members of the Class that their Private Information had been accessed and  
7 compromised.

8 4. Even the most fundamental Private Information, like names, email  
9 addresses, home addresses, or phone numbers, when paired with other uniquely  
10 personalized data like health insurance information, Social Security numbers, and  
11 health plan identification numbers, become especially valuable to cybercriminals to  
12 create seemingly legitimate, personalized phishing scams. The combined exfiltrated  
13 data effectively provides criminals with a key to their personal lives, making it easy  
14 to match additional data, gaining access to their personal and financial accounts and  
15 insight on their preferences. Hackers are now able to build a three-dimensional  
16 picture, and thereby exploit SAG Health’s members.

17 5. SAG Health disregarded the rights of Plaintiffs and Class Members by,  
18 inter alia, failing to take adequate and reasonable measures to ensure its data systems  
19 were protected against unauthorized intrusions; failing to disclose that it did not have  
20 adequately robust computer systems and security practices to safeguard Private  
21 Information; failing to take standard and reasonably available steps to prevent the  
22 Data Breach; and failing to properly train its staff and employees on proper security  
23 measures.

24 6. SAG Health should have ensured that it had adequate monitoring  
25 software in place to detect intrusions or the transfer of large volumes of data to third  
26 party networks, that it implemented multi-factor authentication to verify the  
27 credentials of individuals attempting to access Private Information, that it limited  
28

1 access to Private Information to only necessary employees, that it encrypted or  
2 tokenized Private Information in internet accessible locations, and that it deleted or  
3 redacted Private Information that it was no longer required to maintain. By failing to  
4 implement these reasonable and industry standard data security measures, SAG  
5 Health enabled the unauthorized access of Plaintiffs' and Class Members' Private  
6 Information.

7 7. In addition, SAG Health failed to properly monitor its computer network  
8 and systems that housed the Private Information. Had it properly monitored these  
9 electronic and cloud-based systems, it would have discovered the intrusion sooner or  
10 prevented it altogether.

11 8. The unfortunate reality is that this could have been avoided, had  
12 Defendant taken adequate and reasonable measures to ensure its data systems were  
13 protected against unauthorized intrusions. Instead, it neglected industry standards,  
14 failed to take standard and reasonably available steps to prevent the Data Breach, all  
15 while promising its members advanced security to maintain an advantage in highly  
16 sensitive and competitive industry.

17 9. Equally troubling, SAG Health failed to provide timely and adequate  
18 notice to Plaintiffs and other members of the Class that their Private Information had  
19 been accessed and compromised. Underscoring its grossly negligent business  
20 practices, Defendant waited 3 months before disclosing the Data Breach to SAG-  
21 Health Plan members.

22 10. As a direct and proximate result of Defendant's inadequate security  
23 measures and disclosure of information to an unauthorized criminal third-party,  
24 Plaintiffs and the class suffered several injuries, including (i) out-of-pocket expenses  
25 associated with preventing, detecting, and remediating identity theft, social  
26 engineering, and other unauthorized use of their Private Information; (ii) opportunity  
27 costs associated with attempting to mitigate the actual consequences of the Data  
28 Breach, including but not limited to lost time; (iii) the continued, long term, and

1 certain increased risk that unauthorized persons will access and abuse Plaintiffs' and  
2 Class Members' Private Information; (iv) the continued and certain increased risk that  
3 the Private Information that remains in Defendant's possession is subject to further  
4 unauthorized disclosure for so long as Defendant fails to undertake proper measures  
5 to protect the Private Information; (v) invasion of privacy and disclosure of their  
6 personal information, as well as an increased risk of fraud and identity theft; (vi) theft  
7 of their Private Information and the resulting loss of privacy rights in that information;  
8 (vii) diminution in value and/or lost value of Private Information, a form of property  
9 that Defendant obtained from Plaintiffs and Class Members.

10 11. Plaintiffs bring this lawsuit on behalf of themselves and all those similarly  
11 situated to address Defendant's inadequate safeguarding of Class Members' Private  
12 Information that it collected and maintained. To remedy these violations of law,  
13 Plaintiffs and Class Members thus seek actual damages, statutory damages,  
14 restitution, and injunctive and declaratory relief (including significant improvements  
15 to Defendant's data security protocols and employee training practices), reasonable  
16 attorneys' fees, costs, and expenses incurred in bringing this action, and all other  
17 remedies this Court deems just and proper.

## 18 **II. PARTIES**

### 19 **A. Plaintiff Matthew Rouillard**

20 12. Plaintiff Matthew Rouillard is a citizen and resident of New York, New  
21 York.

22 13. Plaintiff Rouillard entrusted his Private Information to Defendant in  
23 connection with his enrollment and participation in the SAG-AFTRA Health Plan.

24 14. Plaintiff Rouillard received a notice of the Data Breach from Defendant  
25 on December 2, 2024.

26 15. Plaintiff Rouillard only allowed Defendant to maintain, store, and use his  
27 Private Information because he reasonably expected that Defendant would use basic  
28 security measures to protect his Private Information and prevent its access by

1 unauthorized third parties, such as requiring passwords and multi-factor  
2 authentication to access accounts or databases storing his Private Information,  
3 exercising appropriate managerial control to require employee training in recognizing  
4 and thwarting social engineering attacks, and timely disclosing and patching any data  
5 security vulnerabilities. As a result of this expectation, Plaintiff Rouillard entrusted  
6 his Private Information to Defendant, and his Private Information was within the  
7 possession and control of Defendant at the time of the Data Breach.

8 16. Plaintiff Rouillard's Private Information was exposed in the Data Breach.

9 17. As a result of the Data Breach, Plaintiff Rouillard has devoted  
10 considerable time and resources to protect himself from the Data Breach, including  
11 but not limited to researching the Data Breach and monitoring his accounts for  
12 suspicious activity.

13 18. The substantial risk of imminent harm and loss of privacy has also caused  
14 Plaintiff to suffer stress, fear, emotional distress, and anxiety.

15 19. Plaintiff Rouillard has also been injured by the damages to and loss of  
16 value of his Private Information – a form of intangible property that Plaintiff entrusted  
17 to Defendant. This information has inherent value that Plaintiff was deprived of when  
18 his Private Information was negligently made accessible to and intentionally and  
19 maliciously exfiltrated by cybercriminals.

20 20. Given the highly sensitive nature of the information involved, the Data  
21 Breach has also caused Plaintiff Rouillard to suffer imminent harm arising from a  
22 substantially increased risk of additional fraud, identity theft, financial crimes, and  
23 misuse of his Private Information. This highly sensitive information is now in the  
24 hands of criminals as a direct and proximate result of Defendant's misconduct.

25 21. Had Plaintiff Rouillard been informed of Defendant's insufficient data  
26 security measures to protect his Private Information, he would not have willingly  
27 provided his Private Information to Defendant.  
28

**B. Plaintiff Kristy Munden**

22. Plaintiff Kristy Munden is a resident and citizen of Los Angeles, California.

23. Plaintiff Munden entrusted her Private Information to Defendant in connection with her enrollment and participation in the SAG-AFTRA Health Plan.

24. On approximately December 2, 2024, Plaintiff Munden received a notice from Defendant stating her Private Information had been accessed by unauthorized third parties in the Data Breach.

25. Plaintiff Munden only allowed Defendant to maintain, store, and use her Private Information because she reasonably expected that Defendant would use basic security measures to protect her Private Information and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access accounts or databases storing her Private Information, exercising appropriate managerial control to require employee training in recognizing and thwarting social engineering attacks, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Munden entrusted her Private Information to Defendant, and her Private Information was within the possession and control of Defendant at the time of the Data Breach.

26. Plaintiff Munden's Private Information was exposed in the Data Breach.

27. As a result of the Data Breach, Plaintiff Munden has devoted considerable time and resources to protect herself from the Data Breach, including but not limited to researching the Data Breach and monitoring her accounts for suspicious activity.

28. The substantial risk of imminent harm and loss of privacy has also caused Plaintiff to suffer stress, fear, emotional distress, and anxiety.

29. Plaintiff Munden has also been injured by the damages to and loss of value of her Private Information – a form of intangible property that Plaintiff Munden entrusted to Defendant. This information has inherent value that Plaintiff Munden



1 was deprived of when her Private Information was negligently made accessible to and  
2 intentionally and maliciously exfiltrated by cybercriminals.

3 30. Given the highly sensitive nature of the information involved, the Data  
4 Breach has also caused Plaintiff Munden to suffer imminent harm arising from a  
5 substantially increased risk of additional fraud, identity theft, financial crimes, and  
6 misuse of her Private Information. This highly sensitive information is now in the  
7 hands of criminals as a direct and proximate result of Defendant's misconduct.

8 31. Had Plaintiff Munden been informed of Defendant's insufficient data  
9 security measures to protect her Private Information, she would not have willingly  
10 provided her Private Information to Defendant.

11 **C. Plaintiff Lee Wilkof**

12 32. Plaintiff Lee Wilkof is a resident and citizen of Gardiner, New York.

13 33. Plaintiff Wilkof entrusted his Private Information to Defendant in  
14 connection with his enrollment and participation in the SAG-AFTRA Health Plan.

15 34. On approximately December 2, 2024, Plaintiff Wilkof received a notice  
16 from Defendant stating his Private Information had been accessed by unauthorized  
17 third parties in the Data Breach.

18 35. Plaintiff Wilkof only allowed Defendant to maintain, store, and use his  
19 Private Information because he reasonably expected that Defendant would use basic  
20 security measures to protect his Private Information and prevent its access by  
21 unauthorized third parties, such as requiring passwords and multi-factor  
22 authentication to access accounts or databases storing his Private Information,  
23 exercising appropriate managerial control to require employee training in recognizing  
24 and thwarting social engineering attacks, and timely disclosing and patching any data  
25 security vulnerabilities. As a result of this expectation, Plaintiff Wilkof entrusted his  
26 Private Information to Defendant, and his Private Information was within the  
27 possession and control of Defendant at the time of the Data Breach.

28 36. Plaintiff Wilkof's Private Information was exposed in the Data Breach.



1 37. As a result of the Data Breach, Plaintiff Wilkof has devoted considerable  
2 time and resources to protect himself from the Data Breach, including but not limited  
3 to researching the Data Breach and monitoring his accounts for suspicious activity.

4 38. The substantial risk of imminent harm and loss of privacy has also caused  
5 Plaintiff Wilkof to suffer stress, fear, emotional distress, and anxiety.

6 39. Plaintiff Wilkof has also been injured by the damages to and loss of value  
7 of his Private Information – a form of intangible property that Plaintiff Wilkof  
8 entrusted to Defendant. This information has inherent value that Plaintiff Wilkof was  
9 deprived of when his Private Information was negligently made accessible to and  
10 intentionally and maliciously exfiltrated by cybercriminals.

11 40. Given the highly sensitive nature of the information involved, the Data  
12 Breach has also caused Plaintiff Wilkof to suffer imminent harm arising from a  
13 substantially increased risk of additional fraud, identity theft, financial crimes, and  
14 misuse of his Private Information. This highly sensitive information is now in the  
15 hands of criminals as a direct and proximate result of Defendant's misconduct.

16 41. Had Plaintiff Wilkof been informed of Defendant's insufficient data  
17 security measures to protect his Private Information, he would not have willingly  
18 provided his Private Information to Defendant.

19 **D. Plaintiff Steven Barr**

20 42. Plaintiff Steven Barr is a resident and citizen of Los Angeles County,  
21 California.

22 43. Plaintiff Barr entrusted his Private Information to Defendant in  
23 connection with his enrollment and participation in the SAG-AFTRA Health Plan.

24 44. On approximately December 9, 2024, Plaintiff Barr received a notice  
25 from Defendant stating his Private Information had been accessed by unauthorized  
26 third parties in the Data Breach.

27 45. Plaintiff Barr only allowed Defendant to maintain, store, and use his  
28 Private Information because he reasonably expected that Defendant would use basic

1 security measures to protect his Private Information and prevent its access by  
2 unauthorized third parties, such as requiring passwords and multi-factor  
3 authentication to access accounts or databases storing his Private Information,  
4 exercising appropriate managerial control to require employee training in recognizing  
5 and thwarting social engineering attacks, and timely disclosing and patching any data  
6 security vulnerabilities. As a result of this expectation, Plaintiff Barr entrusted his  
7 Private Information to Defendant, and his Private Information was within the  
8 possession and control of Defendant at the time of the Data Breach.

9 46. Plaintiff Barr's Private Information was exposed in the Data Breach.

10 47. As a result of the Data Breach, Plaintiff Barr has devoted considerable  
11 time and resources to protect himself from the Data Breach, including but not limited  
12 to researching the Data Breach and monitoring his accounts for suspicious activity.

13 48. The substantial risk of imminent harm and loss of privacy has also caused  
14 Plaintiff Barr to suffer stress, fear, emotional distress, and anxiety.

15 49. Plaintiff Barr has also been injured by the damages to and loss of value  
16 of his Private Information – a form of intangible property that Plaintiff Barr entrusted  
17 to Defendant. This information has inherent value that Plaintiff Barr was deprived of  
18 when his Private Information was negligently made accessible to and intentionally  
19 and maliciously exfiltrated by cybercriminals.

20 50. Given the highly sensitive nature of the information involved, the Data  
21 Breach has also caused Plaintiff Barr to suffer imminent harm arising from a  
22 substantially increased risk of additional fraud, identity theft, financial crimes, and  
23 misuse of his Private Information. This highly sensitive information is now in the  
24 hands of criminals as a direct and proximate result of Defendant's misconduct.

25 51. Had Plaintiff Barr been informed of Defendant's insufficient data security  
26 measures to protect his Private Information, he would not have willingly provided his  
27 Private Information to Defendant.  
28

**E. Plaintiff Massimiliano Furlan**

52. Plaintiff Massimiliano Furlan is a resident and citizen of Arleta, California.

53. Plaintiff Furlan entrusted his Private Information to Defendant in connection with his enrollment and participation in the SAG-AFTRA Health Plan.

54. On approximately, December 2, 2024, Plaintiff Furlan received a notice from Defendant stating his Private Information had been accessed by unauthorized third parties in the Data Breach.

55. Plaintiff Furlan only allowed Defendant to maintain, store, and use his Private Information because he reasonably expected that Defendant would use basic security measures to protect his Private Information and prevent its access by unauthorized third parties, such as requiring passwords and multi-factor authentication to access accounts or databases storing his Private Information, exercising appropriate managerial control to require employee training in recognizing and thwarting social engineering attacks, and timely disclosing and patching any data security vulnerabilities. As a result of this expectation, Plaintiff Furlan entrusted his Private Information to Defendant, and his Private Information was within the possession and control of Defendant at the time of the Data Breach.

56. Plaintiff Furlan's Private Information was exposed in the Data Breach.

57. As a result of the Data Breach, Plaintiff Furlan has devoted considerable time and resources to protect himself from the Data Breach, including but not limited to researching the Data Breach and monitoring his accounts for suspicious activity.

58. The substantial risk of imminent harm and loss of privacy has also caused Plaintiff Furlan to suffer stress, fear, emotional distress, and anxiety.

59. Plaintiff Furlan has also been injured by the damages to and loss of value of his Private Information – a form of intangible property that Plaintiff Furlan entrusted to Defendant. This information has inherent value that Plaintiff Furlan was

1 deprived of when his Private Information was negligently made accessible to and  
2 intentionally and maliciously exfiltrated by cybercriminals.

3 60. Given the highly sensitive nature of the information involved, the Data  
4 Breach has also caused Plaintiff Furlan to suffer imminent harm arising from a  
5 substantially increased risk of additional fraud, identity theft, financial crimes, and  
6 misuse of his Private Information. This highly sensitive information is now in the  
7 hands of criminals as a direct and proximate result of Defendant's misconduct.

8 61. Had Plaintiff Furlan been informed of Defendant's insufficient data  
9 security measures to protect his Private Information, he would not have willingly  
10 provided his Private Information to Defendant.

11 62. As a result of the Data Breach, Plaintiffs been further injured by the  
12 damages to and loss in value of their Private Information -a form of intangible  
13 property that Plaintiffs entrusted to Defendant. This information has inherent value  
14 that Plaintiffs were deprived of when their Private Information was negligently made  
15 accessible to and intentionally and maliciously exfiltrated by cybercriminals.

16 63. Given the nature of the information involved and the malicious and  
17 intentional means through which the information was stolen, the Data Breach has also  
18 caused Plaintiffs to suffer imminent harm arising from a substantially increased risk  
19 of additional fraud, identity theft, financial crimes, and misuse of their Private  
20 Information. This highly sensitive information, which includes their name, Social  
21 Security number, and information associated with claims and health insurance  
22 information, is now in the hands of criminals as a direct and proximate result of  
23 Defendant's misconduct.

24 64. As a result of the actual harm Plaintiffs have suffered due to the Data  
25 Breach and the imminent and substantial risk of future harm, the Data Breach has  
26 forced Plaintiffs to spend significant time and energy dealing with issues related to  
27 the Data Breach, including self- monitoring their accounts to ensure no fraudulent  
28 activity has occurred, investigating fraudulent activity, alerting their banking services

1 about the breach, and changing identifying information and passwords for their  
2 accounts. Much of the time and energy that Plaintiffs expended, which has been lost  
3 forever and cannot be recaptured, was spent at Defendant's direction.

4 65. The substantial risk of imminent harm and loss of privacy has also caused  
5 Plaintiffs to suffer stress, fear, emotional distress, and anxiety.

6 **F. Defendant SAG-AFTRA Health Plan**

7 66. Defendant SAG-AFTRA Health Plan is a labor-management trust  
8 established under California law, with its principal place of business located in  
9 Burbank, California. Defendant conducts business, providing health benefits to  
10 eligible participants, across the nation.

11 **III. JURISDICTION AND VENUE**

12 67. This Court has subject matter jurisdiction of this action pursuant to 28  
13 U.S.C. Section 1332(d) because this is a class action where the aggregate amount in  
14 controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs,  
15 there are more than 100 members in the proposed class, and at least one Class Member  
16 is a citizen of a state different from Defendant. This Court has supplemental  
17 jurisdiction over any state law claims pursuant to 28 U.S.C. Section 1367.  
18 Furthermore, the affected victims of the data breach – the Class Members – reside  
19 nationwide.

20 68. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action  
21 because a substantial part of the events, omissions, and acts giving rise to the claims  
22 herein occurred in this District: Defendant's principal place of business is located in  
23 this District from where its board of directors and/or officers direct Defendant's  
24 activities including to their actions and inactions leading to the data breach at issue;  
25 Defendant gains revenue and profits from doing business in this District; Class  
26 Members were affected by the breach from SAG Health's actions and inactions  
27 directed from this District.  
28

1 **IV. FACTUAL ALLEGATIONS**

2 69. SAG Health is a provider of health and medical benefits servicing tens of  
3 thousands of SAG-AFTRA members and their families primarily in California and  
4 New York. Defendant collects and processes the personal data of its members. To  
5 avail themselves of benefits coverage, members are forced to entrust Defendant with  
6 their Private Information.

7 70. The information collected and stored by Defendant includes, but is not  
8 limited to, *names, Social Security numbers, and information associated with claims*  
9 *and health insurance information*. Plaintiffs and other similarly situated members  
10 trusted Defendant with their sensitive and valuable Private Information.

11 **A. The Data Breach**

12 71. At all material times, SAG Health failed to maintain proper security  
13 measures despite its promises of safety and security to consumers.

14 72. On September 18, 2024, Defendant became aware that an employee's  
15 email account had been compromised; specifically, on September 16 and 17, there  
16 was unauthorized access to Defendant's internal systems. Defendant did not notify its  
17 customers then, nor made any announcements to alert of this major security issue. By  
18 October 3, 2024, Defendant concluded that members' information was likely  
19 acquired.<sup>3</sup> Yet again, Defendant chose not to notify the affected customers for the  
20 next several months.

21 73. On around December 2, 2024, Defendant finally began notifying some  
22 members of the Data Breach, including Plaintiffs, when nearly three months had  
23 passed since learning of the unauthorized access and two months had passed since  
24 Defendant concluded that personal information had likely been acquired.

25 74. In its December 2 statement, Defendant did not disclose how many  
26 members' Private Information was breached, leaving consumers to speculate whether  
27

28 <sup>3</sup> *SAG-AFTRA Health Plan Email Phishing Notice, supra* fn 2.

1 it is likely that their PII/PHI has been compromised and without any clear instruction  
2 on what they can do to protect themselves now that their Private Information has been  
3 exposed. Instead, Defendant downplayed the extent of the Data Breach, and the likely  
4 harm affected victims may experience.

5 75. Separately and without informing Plaintiffs and the Class, Defendant  
6 notified the U.S. Department Office Health and Human Services Office of Civil  
7 Rights that 35,592 individuals had been affected by the Data Breach.<sup>4</sup>

8 76. Defendant acknowledged the risk posed to Class Members and their  
9 Private Information as a result of the Data Breach, explicitly stating that “We take  
10 this matter very seriously,” encouraging members to “be on alert for any suspicious  
11 activity related to their financial accounts and credit reports” and to “regularly  
12 monitor their credit report, statements, and records to ensure that there are no  
13 transactions or other activities that were not initiated or authorized by them.”

14 **B. Data Breaches and the Market for PII/PHI**

15 77. When a victim’s data is compromised in a breach, the victim is exposed  
16 to serious ramifications regardless of the sensitivity of the data—including but not  
17 limited to identity theft, fraud, decline in credit, inability to access healthcare, as well  
18 as legal consequences.<sup>5</sup> These harms are amplified where, as here, the compromised data  
19 is particularly sensitive.

20 78. The U.S. Department of Justice’s Bureau of Justice Statistics has found  
21 that “among victims who had personal information used for fraudulent purposes, 29%  
22 spent a month or more resolving problems” and that resolution of those problems  
23  
24

25 <sup>4</sup> The State Journal Register, [https://data.sj-r.com/health-care-data-breaches/sag-](https://data.sj-r.com/health-care-data-breaches/sag-afta-health-plan-ca-35592-20241202-hacking-email/)  
26 [afta-health-plan-ca-35592-20241202-hacking-email/](https://data.sj-r.com/health-care-data-breaches/sag-afta-health-plan-ca-35592-20241202-hacking-email/) (last accessed July 31, 2025).

27 <sup>5</sup> Identity Theft Resource Center, 2017 Annual Data Breach Year-End Review,  
28 [https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC\\_2018-End-of-](https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf)  
[Year-Aftermath\\_FINAL\\_V2\\_combinedWEB.pdf](https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf) (last accessed July 31, 2025).



1 could take more than a year.<sup>6</sup>

2 79. The U.S. Government Accountability Office (GAO) has concluded that it  
3 is common for data thieves to hold onto stolen data for extended periods of time  
4 before utilizing it for identity theft.<sup>7</sup> In the same report, the GAO noted that while  
5 credit monitoring services can assist with detecting fraud, those services do not stop  
6 it.<sup>8</sup>

7 80. When entities entrusted with personal data fail to implement industry best  
8 practices, cyberattacks and other data exploitations can go undetected for a long  
9 period of time. This worsens the ramifications and can even render the harm  
10 irreparable.

11 81. PII is a valuable commodity for which a black market exists on the dark  
12 web, among other places. Personal data can be worth from \$1,000-\$1,200 on the dark  
13 web and the legitimate data brokerage industry is valued at more than \$250 billion.<sup>9, 10</sup>

14 82. In fact, “[a] stolen Social Security number is one of the leading causes of  
15  
16

---

17 <sup>6</sup> U.S. Department of Justice, Bureau of Justice Statistics, Victims of Identity Theft,  
18 2014 (Sept. 2015), <http://www.bjs.gov/content/pub/pdf/vit14.pdf> (last accessed July  
19 31, 2025).

20 <sup>7</sup> U.S. Government Accountability Office Report to Congressional Requesters, Data  
21 Breaches – Range of Consumer Risks Highlights Limitations of Identity Theft  
22 Services,  
<https://www.gao.gov/assets/700/697985.pdf> (last accessed July 31, 2025).

23 <sup>8</sup> *Id.*

24 <sup>9</sup> Ryan Smith, *Revealed-how much is personal data worth on the dark web?*,  
INSURANCE BUSINESS MAGAZINE,  
25 [https://www.insurancebusinessmag.com/ca/news/cyber/revealed--how-much-is-](https://www.insurancebusinessmag.com/ca/news/cyber/revealed--how-much-is-personal-data-worth-on-the-dark-web-444455.aspx)  
26 [personal-data-worth-on-the-dark-web-444455.aspx](https://www.insurancebusinessmag.com/ca/news/cyber/revealed--how-much-is-personal-data-worth-on-the-dark-web-444455.aspx) (last accessed July 31, 2025).

27 <sup>10</sup> Maria LaMagna, *The sad truth about how much your Google data is worth on the*  
28 *dark web*, MARKETWATCH (last accessed July 31, 2025). 17 Emily Wilson, *The*  
*Worrying Trend of Children’s Data Being Sold on the Dark Web*, TNW (February  
23, 2019), [https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-](https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark-web/)  
[dark- web/](https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark-web/) (last accessed July 31, 2025).

1 identity theft and can threaten your financial health.”<sup>11</sup> “Someone who has your SSN  
2 can use it to impersonate you, obtain credit and open bank accounts, apply for jobs,  
3 steal your tax refunds, get medical treatment, and steal your government benefits.”<sup>12</sup>

4 83. Medical data is even more valuable because unlike other personal  
5 information, such as credit card numbers which can be quickly changed, medical data  
6 is static. This is why companies possessing medical information, like Defendant, are  
7 targeted by cyber-criminals.<sup>13</sup>

8 84. The greater efficiency of electronic health records brings the risk of  
9 privacy breaches. These electronic health records contain a lot of sensitive  
10 information (e.g., patient data, patient diagnosis, lab results, medications,  
11 prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient’s  
12 complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII  
13 is a valuable commodity for which a “cyber black market” exists where criminals  
14 openly post stolen payment card numbers, Social Security numbers, and other  
15 personal information on several underground internet websites. Unsurprisingly, the  
16 healthcare industry is at high risk and is acutely affected by cyberattacks, like the Data  
17 Breach here.

18 85. “Medical identity theft is a growing and dangerous crime that leaves its  
19 victims with little to no recourse for recovery,” reported Pam Dixon, executive  
20 director of World Privacy Forum. “Victims often experience financial repercussions  
21

22  
23 <sup>11</sup> *How to Protect Yourself from Social Security Number Identity Theft*, EQUIFAX  
24 <https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/> (last accessed July 31, 2025).

25 <sup>12</sup> *What Is an SSN? What to Know About Social Security Numbers*, INVESTOPEDIA  
26 <https://www.investopedia.com/terms/s/ssn.asp> (last accessed July 31, 2025).

27 <sup>13</sup> Caroline Humer & Jim Finkle, *Your medical record is worth more to hackers than your credit card*, REUTERS (September 24, 2014), <https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924> (last accessed July 31, 2025).  
28

1 and worse yet, they frequently discover erroneous information has been added to their  
2 personal medical files due to the thief's activities."<sup>14</sup>

3 86. A 2021 report by Invisibly, a team of application developers focused on  
4 reclaiming users' data, found that personal medical information is one of the most  
5 valuable pieces of information within the market for data. The report noted that "[i]t's  
6 worth acknowledging that because health care records often feature a more complete  
7 collection of the PII User's identity, background, and personal identifying  
8 information (PII), health care records have proven to be of particular value for data  
9 thieves." While a single SSN might go for \$0.53, a complete health care record sells  
10 for \$250 on average.<sup>15</sup>



Record Type	Average Price
Health Care Record	\$250.15
Payment Card Details	\$5.40
Banking Records	\$4.12
Access Credentials	\$0.95
Social Security Number	\$0.53
Credit Record	\$0.31
Basic PII	\$0.03

11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
<sup>14</sup> Michael Ollove, The Rise of Medical Identity Theft in Healthcare, Kaiser Health  
News, Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/>

27  
28  
<sup>15</sup> *How Much is Your Data Worth? The Complete Breakdown for 2024*, INVISIBLY  
(July 13, 2021) <https://www.invisibly.com/learn-blog/how-much-is-data-worth/> (last  
accessed July 31, 2025).

1 87. Medical records are even worth more than an SSN, credit card, and  
2 driver's license combined, according to federal officials. They estimate that medical  
3 records can go for anywhere between \$250 to \$1,000.<sup>16</sup>

4 88. In this black market, criminals seek to sell stolen data to identity thieves  
5 who desire the data to extort and harass victims, take over victims' identities in order  
6 to open financial accounts, and otherwise engage in illegal financial transactions  
7 under the victims' names.

8 89. PII has a distinct, high value—which is why legitimate companies and  
9 criminals seek to obtain and sell it.

10 90. Medical information in particular is extremely valuable to identity thieves  
11 as the medical industry has also experienced disproportionately higher numbers of data  
12 theft events than other industries. According to a report by the Health Insurance  
13 Portability and Accountability Act Journal, "healthcare data breach statistics clearly  
14 show there has been an upward trend in data breaches over the past nine (9) years,  
15 with 2018 seeing more data breaches reported than any other year since records first  
16 started being published."

17 91. A study done by Experian found that the "average total cost" of medical  
18 identity theft is "about \$20,000" per incident, and that most victims of medical  
19 identity theft were forced to pay out of pocket costs for healthcare they did not receive  
20 to restore coverage.<sup>17</sup> Indeed, data breaches and identity theft have a crippling effect  
21 on individuals and detrimentally impact the economy as a whole.

22 92. It should be no surprise that in today's digital economy the "world's most  
23  
24

---

25 <sup>16</sup> Wilkinson, Kate. *RI hospitals fight cyberattacks on 'almost a daily basis'*, WPRI  
26 (Oct. 10, 2023), <https://www.wpri.com/target-12/ri-hospitals-fight-cyberattacks-on-almost-a-daily-basis/> (last accessed July 31, 2025).

27 <sup>17</sup> See Elinor Mills, Study: *Medical Identity theft is costly for victims*, CNET (Mar. 3,  
28 2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last accessed July 31, 2025).

1 valuable resource is no longer oil, but data.”<sup>18</sup> As such, personal information is a  
2 valuable property right.<sup>19</sup> Its value is axiomatic, considering the value of “big data”  
3 in corporate America and the consequences of cyber thefts include heavy prison  
4 sentences. Even this obvious risk to reward analysis illustrates beyond doubt that  
5 personal information has considerable market value.

6 93. In a consumer-driven world, the ability to capture and use consumer data  
7 to shape products, solutions, and the buying experience is critically important to a  
8 business’s success. Research shows that organizations who “leverage customer  
9 behavior insights outperform peers by 85 percent in sales growth and more than 25  
10 percent in gross margin.”<sup>20</sup>

11 94. Indeed, an entire economy exists related to the value of personal data. In  
12 2022, the big data technology market was valued at roughly \$309 billion, and that  
13 value is expected to grow to \$842 billion by 2023.<sup>21</sup>

14 95. In 2013, the Organization for Economic Cooperation and Development  
15 (“OECD”) even published a paper entitled “Exploring the Economics of Personal  
16  
17  
18

---

19 <sup>18</sup> *The world’s most valuable resource is no longer oil, but data*, The Economist (May  
20 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longeroil-but-data>.

21 <sup>19</sup> See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The “Value” of Personally*  
22 *Identifiable Information (“PII”) Equals the “Value” of Financial Assets*, 15 Rich.  
23 J.L. & Tech. 11, at \*3-4 (2009) (“PII, which companies obtain at little cost, has  
quantifiable value that is rapidly reaching a level comparable to the value of  
traditional financial assets.”) (citations omitted).

24 <sup>20</sup> Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing*  
25 *value from your customer data*, McKinsey (Mar. 15, 2017),  
26 <https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data>.

27 <sup>21</sup> Big Data Technology Market Research Report, Fortune Business Insights (Sept.  
28 2023), <https://www.fortunebusinessinsights.com/industry-reports/big-data-technology-market-100144>

1 Data: A Survey of Methodologies for Measuring Monetary Value.”<sup>22</sup> In this paper,  
2 the OECD measured prices demanded by companies concerning user data derived  
3 from “various online data warehouses.”<sup>23</sup> OECD indicated that “[a]t the time of  
4 writing, the following elements of personal data were available for various prices:  
5 USD 0.50 cents for an address, USD 2 [i.e. \$2] for a date of birth, USD 8 for a social  
6 security number (government ID number), USD 3 for a driver’s license number and  
7 USD 35 for a military record. A combination of address, date of birth, social security  
8 number, credit record and military [record] is estimated to cost USD 55.”<sup>24</sup>

9 96. Defendant knew or should have known that Plaintiffs’ and Class  
10 Members’ Private Information is valuable, both to legitimate entities, like Defendant,  
11 and to cybercriminals.

12 97. Defendant knew or should have known that Plaintiffs and Class Members  
13 would reasonably rely upon and trust Defendant’s promises regarding security and  
14 safety of their data and systems, and that their valuable Private Information would be  
15 protected.

16 98. By collecting, using, selling, monitoring, and trafficking Plaintiffs’ and  
17 other members’ Private Information, and failing to protect it by maintaining  
18 inadequate security systems, failing to properly archive the Private Information,  
19 allowing access of third parties, and failing to implement security measures,  
20 Defendant caused harm to Plaintiffs and other SAG Health plan members.

21 **C. The Sensitivity of Members’ Private Information Demands Heightened**  
22 **Protection**

23 99. Entities in the healthcare industry are popular targets for cyberattacks and  
24 require top-tier security measures to protect PII/PHI, especially given that these

25 <sup>22</sup> *Exploring the Economics of Personal Data: A Survey of Methodologies for*  
26 *Measuring Monetary Value*, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013),  
27 <https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf>.

28 <sup>23</sup> *Id.* at 25.

<sup>24</sup> *Id.*



1 databases store sensitive patient records.

2 100. Ponemon Institute, an expert in the annual state of cybersecurity,  
3 indicated in 2020 that organizations storing PHI were top targets for cyber-attacks. In  
4 fact, Defendant has been on notice for years that PHI is a prime target for scammers  
5 due to the amount and value of confidential patient information maintained. In 2019  
6 alone, numerous entities in the healthcare sector suffered high-profile data breaches,  
7 including Quest Diagnostics and LabCorp.

8 101. In a survey released by Ponemon Institute in January 2023, nearly half of  
9 respondents (47%) said their organizations experienced a ransomware attack in the  
10 past two years, up from 43% in 2021. And 45% of respondents reported complications  
11 from medical procedures due to ransomware attacks, up from 36% in 2021.<sup>25</sup>

12 102. Countless victims impacted by the Data Breach now face a constant threat  
13 of being repeatedly harmed, including but not limited to living the rest of their lives  
14 knowing that criminals can compile, build and amass and build profiles on them for  
15 decades – exposing them to a continuing threat of identity theft, disclosure of PII/PHI,  
16 threats, extortion, harassment and phishing scams, and the attendant anxiety from not  
17 knowing how your information will be used when it comes into nefarious individuals’  
18 hands.

19 103. Data breaches of this caliber can result in the exposure of extremely  
20 sensitive information about adults and children’s medical histories, medical  
21 conditions, psychological assessments, psychiatric evaluations, location of  
22 employers, schools, residences, and much more, which poses great dangers on its own  
23 – and more importantly poses a great danger not only to SAG members but their minor  
24 dependents. The FBI has warned that “widespread collection of student data could

25 <sup>25</sup> Southwick, Ron. *California medical group discloses ransomware attack, more than*  
26 *3 million affected*, CHIEF HEALTHCARE EXECUTIVE (10 May 2023),  
27 [https://www.chiefhealthcareexecutive.com/view/california-medical-group-](https://www.chiefhealthcareexecutive.com/view/california-medical-group-discloses-ransomware-attack-more-than-3-million-affected)  
28 [discloses-ransomware-attack-more-than-3-million-affected](https://www.chiefhealthcareexecutive.com/view/california-medical-group-discloses-ransomware-attack-more-than-3-million-affected) (last accessed July 31,  
2025).



1 have privacy and safety implications if compromised or exploited.”<sup>26</sup> Defendant  
2 manages health benefit coverage for its members and their dependents; its failure to  
3 safeguard Private Information puts its members’ children at risk.

4 104. Due to these risks, it is imperative for entities like Defendant to routinely:  
5 (a) monitor for system breaches, cyberattacks and other exploitations; (b) update their  
6 software, security procedures, and firewalls; and (c) make sure its employees are  
7 adequately trained to recognize and thwart social engineering attacks, such as  
8 phishing.

9 **D. Defendant’s Duty to Safeguard Private Information**

10 105. Defendant is responsible for safeguarding the Private Information of tens  
11 of thousands of its members, including PII/PHI of those members’ families.

12 106. Defendant collects, receives, and accesses members’ extensive  
13 individually identifiable information. This Private Information includes names and  
14 Social Security numbers, as well as PHI in the form of health insurance information.

15 107. Defendant was prohibited by the Federal Trade Commission Act (the  
16 “**FTC Act**”) (15 U.S.C. § 45) from engaging in “unfair or deceptive acts or practices  
17 in or affecting commerce.” The Federal Trade Commission (the “**FTC**”) has  
18 concluded that an entity’s failure to maintain reasonable and appropriate data security  
19 for individuals’ sensitive personal information is an “unfair practice” in violation of  
20 the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir.  
21 2015).

22 108. The FTC has brought enforcement actions against entities engaged in  
23 commerce for failing to adequately and reasonably protect customer data, treating the  
24 failure to employ reasonable and appropriate measures to protect against unauthorized  
25 access to confidential consumer data as an unfair act or practice prohibited by Section  
26

27 <sup>26</sup> Education Technologies: *Data Collection and Unsecured Systems Could Pose*  
28 *Risks to Children*, FBI Alert No. I-091318-PSA (Sept. 13, 2018),  
<https://www.ic3.gov/media/2018/180913.aspx> (last accessed July 31, 2025).

1 5 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45. Orders resulting  
2 from these actions further clarify the measures businesses must take to meet their data  
3 security obligations.

4 109. The FTC has promulgated numerous guides for businesses which  
5 highlight the importance of implementing reasonable data security practices.  
6 According to the FTC, the need for data security should be factored into all decision-  
7 making.<sup>27</sup>

8 110. In 2016, the FTC updated its publication, *Protecting Personal*  
9 *Information: A Guide for Business*, which established cybersecurity guidelines for  
10 businesses.<sup>28</sup> The guidelines note that businesses should protect the personal  
11 information that they keep; properly dispose of personal information that is no longer  
12 needed; encrypt information stored on computer networks; understand their network’s  
13 vulnerabilities; and implement policies to correct any security problems.

14 111. The FTC further recommends that entities not maintain PII/PHI longer  
15 than needed for authorization of a transaction; limit access to sensitive data; require  
16 complex passwords to be used on networks; use industry-tested methods for security;  
17 monitor for suspicious activity on the network; and verify that third-party service  
18 providers have implemented reasonable security measures.<sup>29</sup>

19 112. Furthermore, FTC requires that entities like Defendant conduct risk  
20 assessments, implement and periodically review access control, encrypt customer  
21

---

22 <sup>27</sup> Federal Trade Commission, *Start With Security*, available at  
23 [https://www.ftc.gov/system/files/documents/plain-language/pdf0205-](https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf)  
[startwithsecurity.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf) (last accessed July 31, 2025).

24 <sup>28</sup> Federal Trade Commission, *Protecting Personal Information: A Guide for*  
25 *Business*, available at [https://www.ftc.gov/system/files/documents/plain-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136-protecting-personal-information.pdf)  
26 [language/pdf-0136-protecting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136-protecting-personal-information.pdf) (last accessed July 31,  
2025).

27 <sup>29</sup> Federal Trade Commission, *Start With Security*, available at  
28 [https://www.ftc.gov/system/files/documents/plain-language/pdf0205-](https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf)  
[startwithsecurity.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf) (last accessed July 31, 2025).

1 information, implement multi-factor authentication for **anyone accessing customer**  
2 **information within their systems**, dispose of customer information securely,  
3 maintain a log of authorized users' activity and keep an eye out of unauthorized  
4 access, **train employees regarding security awareness**, conduct audits, penetration  
5 testing, and system wide scans regularly to test for publicly known security  
6 vulnerabilities – all of which if had been properly implemented would have allowed  
7 Defendant to prevent this Data Breach.

8 113. Defendant failed to properly implement basic data security practices,  
9 allowing for this social engineering attack to occur, victimizing thousands of people  
10 – by failing to adhere to many of the FTC protocols and allowing access to a hacker  
11 impersonating an employee. Defendant should have a multifaceted security protocol  
12 in place, including a program that adequately trains employees on recognizing and  
13 thwarting phishing and social engineering attacks, monitoring out-of-network emails,  
14 segmenting the network, flagging suspicious domain addresses or content, utilized  
15 multifactor authentication before allowing access to highly sensitive information,  
16 mandating strict compliance with these protocols; mandating regular archiving of  
17 email data/removal of sensitive data from emails to servers; avoiding exchanging any  
18 sensitive data for patients/members over the emails, simulating social engineering  
19 attempts to ensure compliance, increasing spam filtering via email gateways,  
20 implementing strict policies regarding exchange of PII/PHI over emails,  
21 implementing and enforcing appropriate credential/key procedures including finger  
22 print recognition/physical key authentication; monitoring systems 24/7 for any  
23 suspicious activity, encrypting data over the email exchanges. Had Defendant  
24 maintained these and other proper protocols and regularly conducted audits to ensure  
25 its vulnerabilities and training, it would have prevented this Data Breach.

26 114. Moreover, as a HIPAA covered business associate, Defendant is required  
27 to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and  
28 Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health

1 Information”), and Security Rule (“Security Standards for the Protection of Electronic  
2 Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

3 115. These rules establish national standards for the protection of patient  
4 information, including protected health information (“PHI”), defined as “individually  
5 identifiable health information” which either “identifies the individual” or where  
6 there is a “reasonable basis to believe the information can be used to identify the  
7 individual,” that is held or transmitted by a healthcare provider. *See* 45 C.F.R. §  
8 160.103.

9 116. Plaintiffs and Class Members provided their Private Information to SAG  
10 Health with the reasonable expectation and mutual understanding that SAG Health  
11 would comply with its obligations to keep such information confidential and secure  
12 from unauthorized access.

13 117. SAG Health’s failure to provide adequate security measures to safeguard  
14 members’ Private Information is especially egregious because it operates in a field  
15 which has recently been a frequent target of scammers attempting to gain access to  
16 confidential PII/PHI, and it had been targeted by an unauthorized individual before.<sup>30</sup>  
17 SAG Health should have been on notice that it was an attractive target for  
18 cybercriminals in 2019, when it detected unauthorized access on its systems that led  
19 to a threat actor using members’ financial information to make unauthorized  
20 purchases.<sup>31</sup>

## 21 **E. Impact of the Data Breach on Consumers**

22 118. Plaintiffs and the Class have suffered actual harm as a result of  
23 Defendant’s conduct. Defendant failed to institute adequate security measures that led  
24 to a data breach. This breach allowed hackers to access the Private Information,  
25

---

26 <sup>30</sup> *FAQs for Data Privacy Event* (2019), AFTRA Retirement Fund, available at  
27 <https://aftraretirement.org/Home/FAQs/faqs-for-data-privacy-event> (last accessed  
28 July 31, 2025)

<sup>31</sup> *Id.*

1 including *names, Social Security numbers, and health insurance information*, of  
2 Plaintiffs and the Class. Now that the Private Information has been accessed and  
3 absconded with, it is available for criminal elements to sell or trade and will continue  
4 to be at risk for the indefinite future. In fact, the U.S. Government Accountability  
5 Office found that, “once stolen data have been sold or posted on the Web, fraudulent  
6 use of that information may continue for years.”<sup>32</sup>

7 119. Plaintiffs and Class Members are now vulnerable to a full gamut of  
8 cybercrimes, loss in value of their property, and have been forced to take remedial  
9 action, as listed below:

### 10 **Digital Phishing Scams**

11 120. Phishing scammers use emails and text messages to trick people into  
12 giving them their personal information, including but not limited to passwords,  
13 account numbers, and social security numbers. Phishing scams are frequently  
14 successful, and the FBI reported that people lost approximately \$57 million to such  
15 scams in 2019 alone.<sup>33</sup>

16 121. Defendant knew or should have known of the dangers of digital phishing  
17 scams. When Personal Information is employed in a social engineering scheme,  
18 criminals can gain unfettered access to individuals, or corporate databases, as the Data  
19 Breach itself evinces.

20 122. Defendant’s members are now more likely to become victims of digital  
21 phishing attacks because of the compromised information.

### 22 **SIM-Swap**

23 123. The data leak can also lead to SIM-swap attacks against the Class. A SIM-  
24 swap attack occurs when the scammers trick a telephone carrier to porting the victim’s

---

25 <sup>32</sup> See U.S. GOV’T ACCOUNTABILITY OFF. REPORT TO CONGRESSIONAL REQUESTERS  
26 29 2007. <https://www.gao.gov/new.items/d07737.pdf>. (last accessed July 31, 2025).

27 <sup>33</sup> See *How to Recognize and Avoid Phishing Scams*, FTC Consumer Advice,  
28 <https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams> (Last  
accessed July 31, 2025).

1 phone number to the scammer's SIM card. By doing so, the attacker is able to bypass  
2 two-factor authentication accounts, as are used to access cryptocurrency wallets and  
3 other important accounts. The type of personal information that has been leaked poses  
4 a profound tangible risk of SIM-swap attacks for the Class.

5 124. Defendant's members are now more likely to become victims of SIM  
6 Swap attacks because of the released personal information.

7 **Loss of Time**

8 125. As a result of this breach, Plaintiffs and impacted consumers will suffer  
9 unauthorized email solicitations, and experience a significant increase in suspicious  
10 phishing scam activity via email, phone calls, text messages, all following the breach.  
11 In addition, Plaintiffs, as a result of the breach, have spent significant time and effort  
12 researching the breach, monitoring their accounts for fraudulent activity, reviewing  
13 unsolicited emails, texts, and answering telephone calls.

14 **Threat of Identity Theft**

15 126. As a direct and proximate result of Defendant's breach of confidence, and  
16 failure to protect Private Information, Plaintiffs and the Class have also been injured  
17 by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams,  
18 and other misuse of this Private Information, resulting in ongoing monetary loss and  
19 economic harm, loss of value of privacy and confidentiality of the stolen Private  
20 Information, illegal sales of the compromised Private Information on the black  
21 market, mitigation expenses and time spent on credit monitoring, identity theft  
22 insurance, credit freezes/unfreezes, expenses and time spent in initiating fraud alerts,  
23 contacting third parties; decreased credit scores, lost work time, and other injuries.  
24 Defendant, through its misconduct, has enabled numerous bad actors to sell and profit  
25 off of Private Information that belongs to Plaintiffs.

26 **Out of Pocket Costs**

27 127. Plaintiffs are now forced to research and subsequently acquire credit  
28 monitoring and reasonable identity theft defensive services and maintain these

1 services to avoid further impact. Plaintiffs anticipate spending out of pocket expenses  
2 to pay for these services.

3 128. Upon information and belief, Defendant also used Plaintiffs' Private  
4 Information for profit and continued to use Plaintiffs' Private Information to target  
5 Plaintiffs and share their information with various third parties for Defendant's own  
6 benefit.

7 **Diminution in Value of a Valuable Property Right**

8 129. Because personal data is valuable personal property, market exchanges  
9 now exist where internet users like Plaintiffs and Class Members can sell or monetize  
10 their own personal data.

11 130. In fact, the data marketplace is so sophisticated that consumers can  
12 actually sell their non-public information directly to a data broker who in turn  
13 aggregates the information and provides it to legitimate marketers or app  
14 developers.<sup>34</sup> For example, consumers who agree to provide their web browsing  
15 history to the Nielsen Corporation can receive up to \$50.00 a year.<sup>35</sup>

16 131. Accordingly, as a result of the Data Breach, Plaintiffs lost the sale value  
17 of their Private Information and the opportunity to control how it is used. That a threat  
18 actor specifically targeted Defendant demonstrates just how valuable Plaintiffs'  
19 Private Information can be to hackers and the significant value of Plaintiffs' Private  
20 Information to cybercriminals.

21 **Summary of Actual Economic and Noneconomic Damages**

22 132. In sum, Plaintiffs and similarly situated consumers were injured as  
23 follows:

24 a) Theft of their Private Information and the resulting loss of privacy  
25

26 <sup>34</sup> See, e.g., *The Personal Data Revolution*, DATACOUP, <https://datacoup.com/>

27 <sup>35</sup> Nielsen Computer & Mobile Panel, *Frequently Asked Questions*,  
28 <https://computermobilepanel.nielsen.com/ui/US/en/faqen.html> (last accessed July 31,  
2025).



rights in that information;

b) Improper disclosure of their Private Information;

c) Loss of value of their Private Information;

d) The amount of ongoing reasonable identity defense and credit monitoring services made necessary as mitigation measures;

e) Defendant's retention of profits attributable to Plaintiffs' and other customers' Private Information that Defendant failed to adequately protect;

f) Economic and non-economic impacts that flow from imminent, and ongoing threat of fraud and identity theft to which Plaintiffs are now exposed;

g) Ascertainable out-of-pocket expenses and the value of Plaintiffs' time allocated to fixing or mitigating the effects of this data breach;

h) Overpayments for Defendant's products and/or services which Plaintiffs paid to enroll in;

i) Emotional distress, and fear associated with the imminent threat of harm from the continued phishing scams and attacks as a result of this data breach.

**F. Defendant Should Have Invested in Appropriate & Necessary Data Security**

133. In the years immediately preceding the Data Breach, Defendant knew or should have known that its computer systems were a target for cybersecurity attacks.

134. The Data Breach was reasonably foreseeable to SAG Health give its close administrative relationship with the AFTRA Retirement Fund ("AFTRA Fund"), which experienced its own data breach in October 2019. Indeed, SAG-Health and the AFTRA-Fund share multiple board trustees, including J. Keith Gorham, Marc

1 Sandman, and David White.<sup>36</sup>

2 135. Like the September 2024 Data Breach SAG-Health experienced, the  
3 AFTRA Fund breach compromised names, Social Security numbers, addresses, and  
4 dates of birth through unauthorized network access that went undetected for several  
5 days.<sup>37</sup> And much like SAG Health, despite discovering the breach in October 2019,  
6 the AFTRA Fund did not notify retirement fund participants until December 2020—  
7 over a year later.<sup>38</sup>

8 136. With shared governance and direct knowledge of the AFTRA Fund's  
9 security failures through common trustees, SAG Health was uniquely positioned to  
10 implement appropriate measures to prevent the Data Breach. Moreover, given that  
11 SAG Health stores identical types of sensitive data as the AFTRA Fund, it had every  
12 reason to prioritize cybersecurity improvements after witnessing the AFTRA Fund's  
13 breach and its consequences.

14 137. But even without such knowledge, SAG Health had reason to foresee the  
15 threats posed by email phishing attacks. The FBI and CISA have issued numerous  
16 warnings about email phishing attacks targeting healthcare and benefits  
17 organizations, with industry standards recognizing email security as a critical  
18 vulnerability requiring employee training, multi-factor authentication, and access  
19 controls. Yet SAG Health still suffered a breach through a compromised employee  
20 email credential—the most basic and preventable attack vector—demonstrating a  
21 shocking failure to implement fundamental safeguards that any reasonable healthcare  
22 entity would have adopted, especially after seeing a sister organization fall victim to  
23

---

24 <sup>36</sup> SAG-AFTRA, *Notice of Data Breach Affecting Pension/Retirement Participants*,  
25 [https://www.sagaftra.org/notice-data-breach-affecting-pensionretirement-](https://www.sagaftra.org/notice-data-breach-affecting-pensionretirement-participants)  
participants (last accessed July 31, 2025).

26 <sup>37</sup> *Compare* SOLIDARITY.US, <https://solidarity.us/sag-aftra-health-plan-trustees>  
27 (last accessed July 31, 2025), *with* SOLIDARITY.US, [https://solidarity.us/aftra-](https://solidarity.us/aftra-retirement-fund-trustees)  
retirement-fund-trustees (last accessed July 31, 2025).

28 <sup>38</sup> *See supra* note 8.

1 cybercriminals.

2 138. The FBI, FTC, GAO, U.S. Secret Service, United States Cybersecurity  
3 and Infrastructure Security Agency, State Attorney General Offices and many other  
4 government and law enforcement agencies, and hundreds of private cybersecurity and  
5 threat intelligence firms, have issued warnings that put Defendant on notice, long  
6 before the Data Breach, that (1) cybercriminals were targeting companies who store  
7 personal health information, such as Defendant; (2) cybercriminals were ferociously  
8 aggressive in their pursuit of large collections of Private Information like that in  
9 possession of Defendant; (3) cybercriminals were selling large volumes of Private  
10 Information and corporate information on Dark Web portals; and (4) the threats were  
11 increasing.

12 139. Had Defendant been diligent and responsible, it would have known about  
13 and acted upon warnings published in 2017 that 93% of data security breaches were  
14 avoidable and the key avoidable causes for data security incidents are:

- 15 • Lack of a complete risk assessment, including internal, third-
- 16 • party, and cloud-based systems and services;
- 17 • Not promptly patching known/public vulnerabilities, and not
- 18 • having a way to process vulnerability reports;
- 19 • Misconfigured devices/servers;
- 20 • Unencrypted data and/or poor encryption key management and
- 21 • safeguarding;
- 22 • Use of end-of-life (and thereby unsupported) devices, operating
- 23 • systems, and applications;
- 24 • Employee errors and accidental disclosures — lost data, files,
- 25 • drives, devices, computers, improper disposal;
- 26 • Failure to block malicious email; and
- 27 • **Users succumbing to business email compromise (BEC) and**
- 28 • **social exploits.**<sup>39</sup>

23 140. In light of the information and warnings readily available to Defendant  
24 before the Data Breach, Defendant had reason to be on guard and to increase data  
25

---

26 <sup>39</sup> Gretel Egan, *OTA Report Indicates 93% of Security Breaches Are Preventable*,  
27 PROOFPOINT (Feb. 7, 2018), available at [https://www.proofpoint.com/us/security-](https://www.proofpoint.com/us/security-awareness/post/ota-report-indicates-93-security-breaches-are-preventable)  
28 [awareness/post/ota-report-indicates-93-security-breaches-are-preventable](https://www.proofpoint.com/us/security-awareness/post/ota-report-indicates-93-security-breaches-are-preventable) (last  
accessed July 31, 2025).

1 security to avoid an attack.

2 141. Further, Defendant suffered a data breach in 2019, yet did not employ  
3 sufficient remedial measures to prevent additional breaches in the future.

4 142. Prior to the Data Breach, Defendant thus knew or should have known that  
5 there was a foreseeable risk that Plaintiffs' and Class Members' Private Information  
6 could be accessed, exfiltrated and utilized by nefarious individuals as the result of a  
7 cyberattack.

8 143. Prior to the Data Breach, Defendant knew or should have known that it  
9 should ensure its employees with access to the Private Information are adequately  
10 trained in recognizing and thwarting social engineering attacks, such as the phishing  
11 attack which led to the Data Breach.

12 144. Data security experts advise that "the vast majority of data breaches are  
13 preventable" if companies follow widely-available advice on data security practices,  
14 including "continually audit[ing] and reevaluat[ing]" their data security practices;  
15 being aware of and working proactively to counter cybercriminals' evolving  
16 techniques and approaches; and training and re-training their employees.<sup>40</sup>

17 145. Defendant did not follow this advice; nor did it otherwise remedy the  
18 inadequacies that it knew led to the first breach of its systems. On its own website,  
19 Defendant provides the link to Online Security Tips posted by the U.S. Department  
20 of Labor, including the requirement to use strong and unique password, avoid using  
21 repeat passwords, changing passwords frequently, using Multi-factor authentication,  
22 keeping personal contact information current, deleting/closing unused accounts,  
23 avoiding Wi-Fi networks, being vigilant of phishing attacks, avoiding clicking  
24 links/providing information to unverified entities even if they appear to look like  
25

---

26 <sup>40</sup> Nate Nead, *How To Prevent A Data Breach In Your Company*, FORBES BUSINESS  
27 COUNSEL, FORBES (Jul. 30, 2021) available at  
28 <https://www.forbes.com/sites/forbesbusinesscouncil/2021/07/30/how-to-prevent-a-data-breach-in-your-company/?sh=3828f7b918da> (last accessed July 31, 2025).

1 trusted organizations, and other similar tips. Had Defendant enforced strict  
2 compliance with these tips, this Data Breach would have been preventable.

3 **V. CLASS ALLEGATIONS**

4 146. Plaintiffs bring this case individually and, pursuant to Rule 23(b)(2),  
5 (b)(3), and (c)(4) of the Federal Rules of Civil Procedure, on behalf of the following  
6 Nationwide Class and State Classes (collectively the “Class”):

7 **Nationwide Class**

8 “All persons whose Private Information was  
9 accessed, compromised, or stolen in the Data Breach  
10 announced by Defendant on December 2, 2024” (the  
11 “Class”).

12 **California Subclass**

13 “All persons who currently reside in California and  
14 whose Private Information was accessed,  
15 compromised, or stolen in the data breach announced  
16 by Defendant on December 2, 2024” (the “California  
17 Subclass”).

18 147. Excluded from the Class is Defendant, its subsidiaries and affiliates, its  
19 officers, directors and members of their immediate families and any entity in which  
20 Defendant has a controlling interest, the legal representative, heirs, successors, or  
21 assigns of any such excluded party, the judicial officer(s) to whom this action is  
22 assigned, and the members of their immediate families.

23 148. Plaintiffs reserve the right to modify or amend the definition of the  
24 proposed Class, if necessary, before this Court determines whether certification is  
25 appropriate.

26 149. **Numerosity:** The Class is comprised of tens of thousands of SAG-  
27 AFTRA Health Plan members throughout the United States and the state of California  
28 (the “Class Members”). The Class is so numerous that joinder of all members is  
impracticable and the disposition of their claims in a class action will benefit the  
parties and the Court.

1           150. **Predominance of Common Questions:** Common questions of law and  
2 fact exist as to all members of the Class and predominate over any questions affecting  
3 solely individual members of the Class. Among the questions of law and fact common  
4 to the Class that predominate over questions which may affect individual Class  
5 members, including the following:

- 6           a. Whether Defendant's conduct is in violation of Business and  
7           Professions Code section 17200, *et seq.*;
- 8           b. Whether Defendant's conduct is in violation of California Civil Code  
9           §§ 1798, *et seq.*;
- 10          c. Whether Defendant's conduct is in violation of California Civil Code  
11          §§ 56, *et seq.*;
- 12          d. Whether Defendant's conduct is in violation of California Civil Code  
13          §§ 1798.100, *et. seq.*;
- 14          e. Whether Defendant's failure to implement effective security measures  
15          to protect Plaintiffs' and the Class's Private Information was  
16          negligent;
- 17          f. Whether Defendant owed a duty to Plaintiffs and the Class to exercise  
18          due care in collecting, storing, and safeguarding their Private  
19          Information;
- 20          g. Whether Defendant breached a duty to Plaintiffs and the Class to  
21          exercise due care in collecting, storing, and safeguarding their Private  
22          Information;
- 23          h. Whether Class Members' Private Information was accessed,  
24          compromised, or stolen in the Data Breach;
- 25          i. Whether Defendant's conduct caused or resulted in damages to  
26          Plaintiffs and the Class;
- 27          j. Whether Defendant failed to notify the public of the breach in a timely  
28          and adequate manner;

1 k. Whether Defendant knew or should have known that its systems,  
2 including but not limited to training protocols and policies, left it  
3 vulnerable to a data breach;

4 l. Whether Defendant adequately addressed the vulnerabilities that  
5 allowed for the Data Breach; and

6 m. Whether, as a result of Defendant's conduct, Plaintiffs and the Class  
7 are entitled to damages and relief.

8 151. **Typicality:** Plaintiffs' claims are typical of the claims of the proposed  
9 Class, as Plaintiffs and Class Members were harmed by Defendant's uniform  
10 unlawful conduct.

11 152. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the  
12 interests of the proposed Class. Plaintiffs have retained competent and experienced  
13 counsel in class action and other complex litigation.

14 153. The Class is identifiable and readily ascertainable. Notice can be provided  
15 to such purchasers using techniques and a form of notice similar to those customarily  
16 used in class actions, and by internet publication, radio, newspapers, and magazines.

17 154. **Superiority:** A class action is superior to other available methods for fair  
18 and efficient adjudication of this controversy. The expense and burden of individual  
19 litigation would make it impracticable or impossible for proposed members of the  
20 Class to prosecute their claims individually.

21 155. The litigation and resolution of the Class's claims are manageable.  
22 Individual litigation of the legal and factual issues raised by Defendant's conduct  
23 would increase delay and expense to all parties and the court system. The class action  
24 device presents far fewer management difficulties and provides the benefits of a  
25 single, uniform adjudication, economies of scale, and comprehensive supervision by  
26 a single court.

27 156. Defendant has acted on grounds generally applicable to the entire Class,  
28 thereby making final injunctive relief and/or corresponding declaratory relief



1 appropriate with respect to the Class as a whole. The prosecution of separate actions  
2 by individual Class Members would create the risk of inconsistent or varying  
3 adjudications with respect to individual member of the Class that would establish  
4 incompatible standards of conduct for Defendant.

5 157. Absent a class action, Defendant will likely retain the benefits of its  
6 wrongdoing. Because of the small size of the individual Class Members' claims, few,  
7 if any, Class Members could afford to seek legal redress for the wrongs complained  
8 of herein. Absent a representative action, Class Members will continue to suffer losses  
9 and Defendant (and similarly situated companies) will be allowed to continue these  
10 violations of law and to retain the proceeds of its ill-gotten gains.

11 **COUNT ONE**

12 **VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW**

13 **BUSINESS & PROFESSIONS CODE SECTION 17200, *et seq.***

14 **(By All Plaintiffs on Behalf Nationwide Class)**

15 158. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege  
16 and fully incorporate all allegations in all preceding paragraphs.

17 159. California Business and Professions Code Section 17200, *et seq.*,  
18 identifies violations of any state or federal law as "unlawful practices that the unfair  
19 competition law makes independently actionable." *Velazquez v. GMAC Mortg. Corp.*,  
20 605 F. Supp. 2d 1049, 1068 (C.D. Cal. 2008).

21 160. Defendant's unlawful conduct, as alleged in the preceding paragraphs,  
22 violates California Civil Code Section 1750, *et seq.*

23 161. Defendant has engaged in "unlawful" business practices by violating  
24 multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§  
25 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring  
26 timely breach notification), the FTC Act, 15 U.S.C. § 45, California's Confidentiality  
27 of Medical Information Act, Cal. Civ. Code § 56, California's Consumer Privacy Act,  
28 Cal. Civ. Code § 1798.100, and California common law.

1 162. Plaintiffs' harm and injuries alleged herein was the direct and proximate  
2 result of Defendant's unlawful and wrongful conduct, all of which occurred within  
3 the State of California.

4 163. Defendant knew or should have known of its unlawful conduct.

5 164. Defendant could have furthered its legitimate business interests in ways  
6 other than by its unlawful conduct.

7 165. All of the conduct alleged herein occurs and continues to occur in  
8 Defendant's business. Defendant's unlawful conduct is part of a pattern or  
9 generalized course of conduct repeated on approximately thousands of occasions  
10 daily.

11 166. Pursuant to Business and Professions Code Sections 17203, Plaintiffs and  
12 the Class seek an order of this Court enjoining Defendant from continuing to engage,  
13 use, or employ its unlawful business practices.

14 167. Plaintiffs and the Class have suffered injury-in-fact and have lost money  
15 or property as a result of Defendant's unfair conduct. Plaintiffs and the Class would  
16 not have given Defendant their Private Information, had they known that their Private  
17 Information was vulnerable to a data breach. Additionally, SAG Health members paid  
18 money, directly or indirectly to SAH Health in return for membership benefits.  
19 Defendant should have applied a portion of that money to data security but instead  
20 directed it to its own profit. Likewise, Plaintiffs and Class Members seek an order  
21 mandating that Defendant implement adequate security practices to protect members'  
22 Private Information. Additionally, Plaintiffs and the members of the Class seek and  
23 request an order awarding Plaintiffs and the Class restitution of the money wrongfully  
24 acquired by Defendant by means of Defendant's unfair and unlawful practices.

25 168. **Injunction.** Pursuant to Business and Professions Code Sections 17203,  
26 Plaintiffs and the Class seek an order of this Court compelling Defendant to  
27 implement adequate safeguards to protect consumer Private Information retained by  
28 Defendant. This includes, but is not limited to: improving security systems, deleting

1 data that no longer needs to be retained by Defendant, archiving that data on secure  
2 servers, adopting adequate and robust training policies and protocols for all  
3 employees entrusted with access to Personal Information and notifying all affected  
4 consumers in a timely manner.

5 169. No adequate remedy at law. Plaintiffs and the Class are entitled to  
6 equitable relief as no adequate remedy at law exist because:

- 7 a) Defendant has not yet implemented adequate protections to prevent a  
8 future data breach, nor has it given an adequate notice to all affected  
9 class members, and therefore, the equitable relief requested here  
10 would prevent ongoing and future harm;
- 11 b) The equitable relief under the UCL (and also under unjust enrichment  
12 discussed below) creates a straightforward cause of action for  
13 violations of law (such as statutory or regulatory requirements related  
14 to representations and omissions made with respect to Defendant's  
15 services). Furthermore, damages for non-UCL claims require  
16 additional elements or pre-suit notice letters, which would potentially  
17 eliminate possibility of providing damages to the entire class, while  
18 restitution would provide certainty and remedy for all affected victims.
- 19 c) In addition, discovery—which has not yet been provided and/or  
20 completed—may reveal that the claims providing legal remedies are  
21 inadequate. At this time, forcing an election of remedies at the initial  
22 pleadings stage, in the absence of completed discovery regarding class  
23 certification and merits, is premature and likely to lead to subsequent,  
24 potentially belated, and hotly contested motions to amend the  
25 pleadings to add equitable remedies based on a lengthy historical  
26 recount of discovery and analysis of voluminous exhibits, transcripts,  
27 discovery responses, document productions, etc., as well as related  
28 motions to seal confidential information contained therein.

**COUNT TWO**

**NEGLIGENCE**

**(By All Plaintiffs on Behalf of the Nationwide Class)**

170. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

171. Defendant owed a duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information. This duty included but was not limited to: (a) designing, implementing, and testing security systems to ensure that consumers' Private Information was consistently and effectively protected; (b) implementing security systems that are compliant with state and federal mandates; (c) implementing security systems that are compliant with industry practices; and (d) promptly detecting and notifying affected parties of a data breach.

172. Defendant's duties to use reasonable care arose from several sources, including those described below. Defendant had a common law duty to prevent foreseeable harm to others, including Plaintiffs and Class Members, who were the foreseeable and probable victims of any inadequate security practices.

173. Defendant had a special relationship with Plaintiffs and Class Members, which is recognized by laws and regulations, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to class members from a data breach. Plaintiffs and Class Members were compelled to entrust Defendant with their PII/PHI. At relevant times, Plaintiffs and Class members understood that Defendant would take adequate security precautions to safeguard that information. Only Defendant had the ability to protect Plaintiffs' and Class Members' PII/PHI stored on its servers.

174. Defendant knew or should have known that Plaintiffs' and the Class Members' Private Information is information that is frequently sought after by criminals.

1 175. Defendant knew or should have known that Plaintiffs and the Class  
2 members would suffer harm if their Private Information was leaked.

3 176. Defendant knew or should have known that its security systems were not  
4 adequate to protect Plaintiffs' and the Class Members' Private Information from a  
5 data breach.

6 177. Defendant knew or should have known that adequate and prompt notice  
7 of the data breach was required such that Plaintiffs and the Class could have taken  
8 more swift and effective action to change or otherwise protect their Private  
9 Information. Defendant failed to provide timely notice upon discovery of the data  
10 breach. Some Class Members were informed of the data breach on December 2, 2024.  
11 Defendant had learned of the data breach more than two months prior, in September  
12 2024, and learned that consumers' PII was compromised over a month prior, in  
13 October 2024.

14 178. Defendant's conduct as described above constituted an unlawful breach  
15 of its duty to exercise due care in collecting, storing, and safeguarding Plaintiffs' and  
16 the Class Members' Private Information by failing to design, implement, and maintain  
17 adequate security measures to protect this information. Moreover, Defendant did not  
18 implement, design, or maintain adequate measures to detect a data breach when it  
19 occurred.

20 179. Defendant's conduct as described above constituted an unlawful breach  
21 of its duty to provide adequate and prompt notice of the data breach.

22 180. Plaintiffs' and the Class Members' Private Information would have  
23 remained private and secure had it not been for Defendant's wrongful and negligent  
24 breach of its duties. The leak of Plaintiffs' and the Class Members' Private  
25 Information, and all subsequent damages, was a direct and proximate result of  
26 Defendant's negligence.

27 181. Defendant's negligence was, at least, a substantial factor in causing  
28 Plaintiffs' and the Class's Private Information to be improperly accessed, disclosed,

1 and otherwise compromised, and in causing Class Members' other injuries arising out  
2 of the Data Breach.

3 182. The damages suffered by Plaintiffs and the Class was the direct and  
4 reasonably foreseeable result of Defendant's negligent breach of its duties to  
5 adequately design, implement, and maintain security systems to protect Plaintiffs' and  
6 Class Members' Private Information. Defendant knew or should have known that its  
7 security for safeguarding Plaintiffs' and Class Members' Private Information was  
8 inadequate and vulnerable to a data breach.

9 183. Defendant's negligence directly caused significant harm to Plaintiffs and  
10 the Class.

11 **COUNT THREE**

12 **INVASION OF PRIVACY**

13 **(By All Plaintiffs on Behalf of the Nationwide Class)**

14 184. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege  
15 and fully incorporate all allegations in all preceding paragraphs.

16 185. Plaintiffs and Class Members had a reasonable and legitimate expectation  
17 of privacy in their Private Information that Defendant failed to adequately protect  
18 against compromise from unauthorized third parties.

19 186. Defendant owed a duty to Plaintiffs and Class Members to keep their  
20 Private Information confidential.

21 187. Defendant failed to protect, and released to unknown and unauthorized  
22 third parties, the Private Information of Plaintiffs and Class Members.

23 188. By failing to keep Plaintiffs' and Class Members' Private Information  
24 safe, knowingly utilizing unsecure systems and practices, Defendant unlawfully  
25 invaded Plaintiffs' and Class Members' privacy by, among others, (i) intruding into  
26 Plaintiffs' and Class Members' private affairs in a manner that would be highly  
27 offensive to a reasonable person; (ii) failing to adequately secure their Private  
28 Information from disclosure to unauthorized persons and/or third parties; and (iii)

1 enabling the disclosure of Plaintiffs' and Class Members' Private Information without  
2 consent.

3 189. Defendant knew, or acted with reckless disregard of the fact that, a  
4 reasonable person in Plaintiffs' and Class Members' position would consider its  
5 actions highly offensive.

6 190. Defendant knew, or acted with reckless disregard of the fact that,  
7 organizations handling PHI are highly vulnerable to cyberattacks and that employing  
8 inadequate security and training practices would render them especially vulnerable to  
9 data breaches.

10 191. As a proximate result of such unauthorized disclosures, Plaintiffs' and  
11 Class Members' reasonable expectations of privacy in their Private Information was  
12 unduly frustrated and thwarted, thereby causing Plaintiffs and the Class Members'  
13 undue harm.

14 192. Plaintiffs seek injunctive relief on behalf of the Class, restitution, as well  
15 as any and all other relief that may be available at law or equity. Unless and until  
16 enjoined, and restrained by order of this Court, Defendant's wrongful conduct will  
17 continue to cause irreparable injury to Plaintiffs and Class Members. Plaintiffs and  
18 Class Members have no adequate remedy at law for the injuries in that a judgment for  
19 monetary damages will not end the invasion of privacy for Plaintiffs and the class.

20 **COUNT FOUR**

21 **VIOLATION OF CALIFORNIA CONFIDENTIALITY OF MEDICAL**  
22 **INFORMATION ACT, CALIFORNIA CIVIL CODE SECTION 56, *et seq.***  
23 **(By Plaintiffs Munden, Barr, and Furlan, on Behalf of the California Subclass)**

24 193. Plaintiffs Munden, Barr, and Furlan (together, "California Plaintiffs"),  
25 individually and on behalf of the California Subclass, herein repeat, reallege and fully  
26 incorporate all allegations in all preceding paragraphs.

27 194. Defendant is subject to the requirements and mandates of the CMIA  
28 because it is a "health care service plan" pursuant to Cal. Civ. Code § 56.10.



1 195. CMIA section 56.36 allows an individual to bring an action against a  
2 “person or entity who has negligently released confidential information or records  
3 concerning him or her in violation of this part.”

4 196. As a direct result of its negligent failure to adequately protect the data it  
5 collected from the California Plaintiffs and California Subclass Members, Defendant  
6 allowed for a Data Breach which released the PII/PHI of Plaintiffs and the Class  
7 Members to criminals and/or third parties.

8 197. The CMIA defines “medical information” as “any individually  
9 identifiable information, in electronic or physical form, in possession of or derived  
10 from a provider of health care ... regarding a patient's medical history, mental or  
11 physical condition, or treatment.”

12 198. The CMIA defines individually identifiable information as “medical  
13 information [that] includes or contains any element of personal identifying  
14 information sufficient to allow identification of the individual, such as the  
15 [customers]’ name, address, electronic mail address, telephone number, or social  
16 security number, or other information that, alone or in combination with other  
17 publicly available information, reveals the individual's identity.” Cal. Civ. Code §  
18 56.050.

19 199. Defendant is in possession of affected individuals’ medical insurance and  
20 claim information, including, but not necessarily limited to, diagnosis and treatment  
21 of patients/customers, laboratory test results, prescription data, radiology reports, and  
22 health plan member numbers, with which more data can be ascertained. Further, the  
23 compromised data was individually identifiable because it was accompanied by  
24 elements sufficient to allow identification of California Plaintiffs by the third parties  
25 to whom the data was disclosed. California Subclass Members’ names were included  
26 in the compromised data.

27 200. Defendant came into possession of California Plaintiffs’ and California  
28 Subclass Members’ medical information and had a duty pursuant to Section 56.06

1 and 56.101 of the CMIA to maintain, store and dispose of the California Plaintiffs'  
2 and California Subclass Members' medical records in a manner that preserved their  
3 confidentiality. Sections 56.06 and 56.101 of the CMIA prohibit the negligent  
4 creation, maintenance, preservation, store, abandonment, destruction, or disposal of  
5 confidential medical information.

6 201. Defendant further violated the CMIA by failing to use reasonable care,  
7 and in fact, negligently maintained California Plaintiffs' and California Subclass  
8 Members' medical information, allowing and enabling a threat actor to view and  
9 access unencrypted PHI for California Plaintiffs and the California Subclass.  
10 California Plaintiffs' PHI has been misused as a result of Defendant's failure to  
11 maintain reasonable security measures and care.

12 202. Since Defendant maintained California Plaintiffs' and California  
13 Subclass Members' medical information in California, on California-based servers,  
14 where it was ultimately disclosed to third parties, CMIA equally applies to the entire  
15 affected Class. *See, e.g., Doe v. Meta Platforms, Inc.*, No. 22-cv-03580-WHO, 2023  
16 U.S. Dist. LEXIS 158683, at \*16 (N.D. Cal. Sep. 7, 2023) (holding that another  
17 statute, CIPA, could apply to non-residents of California, because the conduct at issue  
18 occurred in California).

19 203. As a direct and proximate result of Defendant's violations of the CMIA,  
20 California Plaintiffs and California Subclass Members have been injured and are  
21 entitled to compensatory damages, punitive damages, and nominal damages of one-  
22 thousand dollars (\$1,000) for each of Defendant's violations of the CMIA, as well as  
23 attorneys' fees and costs pursuant to Cal. Civ. Code § 56.36.

24 **COUNT FIVE**

25 **VIOLATIONS OF CALIFORNIA'S CONSUMER PRIVACY ACT,**

26 **CALIFORNIA CIVIL CODE §§ 1798.100, *et. seq.***

27 **(By Plaintiffs Munden, Barr, and Furlan, on Behalf of the California Subclass)**

28 204. California Plaintiffs, individually and on behalf of the California

1 Subclass, herein repeat, reallege and fully incorporate all allegations in all preceding  
2 paragraphs.

3 205. Defendant violated California Civil Code § 1798.150 of California's  
4 Consumer Privacy Act ("CCPA") by failing to implement and maintain reasonable  
5 security procedures and practices appropriate to the nature of the information to  
6 protect the nonencrypted PII of Plaintiffs and the Class. As a direct and proximate  
7 result, California Plaintiffs' and California Subclass Members' unencrypted and  
8 unredacted PII was subject to unauthorized access and theft.

9 206. Defendant is a "business" under the meaning of California Civil Code §  
10 1798.140 because Defendant is a "corporation, association, or other legal entity that  
11 is organized or operated for the profit or financial benefit of its shareholders or other  
12 owners" that "collects consumers' personal information" and is active "in the State of  
13 California" and "had annual gross revenues in excess of twenty-five million dollars  
14 (\$25,000,000) in the preceding calendar year." Civil Code § 1798.140(d).

15 207. California Plaintiffs seek injunctive or other equitable relief to ensure  
16 Defendant hereinafter adequately safeguards Private Information by implementing  
17 reasonable security procedures and practices. Such relief is particularly important  
18 because Defendant continues to hold PII belonging to California Plaintiffs and  
19 California Subclass. California Plaintiffs and the California Subclass have an ongoing  
20 interest in ensuring that their PII is reasonably protected, and Defendant has  
21 demonstrated a pattern of failing to adequately safeguard this information.

22 208. On December 13, 2024, Plaintiff Furlan mailed a CCPA notice letter to  
23 Defendant's principal place of business pursuant to California Civil Code §  
24 1798.150(b), detailing the specific provisions of the CCPA that Defendant has  
25 violated and continues to violate. Defendant has not provided Plaintiff Furlan with an  
26 express written statement that the violations have been cured and that no further  
27 violations shall occur. Accordingly, seeks all damages and appropriate equitable relief  
28 available under the CCPA on behalf of himself and the California Subclass members.

209. On December 10, 2024, Plaintiff Barr mailed a CCPA notice letter to Defendant's principal place of business pursuant to California Civil Code § 1798.150(b), detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. Defendant has not provided Plaintiff Barr with an express written statement that the violations have been cured and that no further violations shall occur. Accordingly, Plaintiff Barr seeks all damages and appropriate equitable relief available under the CCPA on behalf of himself and the California Subclass members.

210. On July 31, 2025, Plaintiff Munden mailed a CCPA notice letter to Defendant's registered service agents Pursuant to California Civil Code § 1798.150(b), detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant does not provide express written statement within 30 days that its CCPA violations have been cured and that no further violations shall occur, Plaintiff Munden will amend her CCPA claim to seek statutory damages under the CCPA. At this time, California Plaintiff Munden only seeks actual pecuniary damages for Defendant's violations of the CCPA.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, pray for judgment and relief on all causes of action as follows:

1. That the Court determines that this Action may be maintained as a Class Action, that Plaintiffs be named as Class Representatives of the Class, that the undersigned be named as Class Counsel of the Class, and that notice of this Action be given to Class Members;
2. That the Court enter an order declaring that Defendant's actions, as set forth in this Complaint, violate the laws set forth above;
3. An order:
  - a) Prohibiting Defendant from engaging in the wrongful acts stated herein (including Defendant's utter failure to provide

- notice to all affected consumers);
- b) Requiring Defendant to implement adequate security protocols and practices to protect consumers' Private Information consistent with the industry standards, applicable regulations, and federal, state, and/or local laws;
  - c) Mandating the proper notice be sent to all affected consumers, and posted publicly;
  - d) Requiring Defendant to protect all data collected through any account creation requirements;
  - e) Requiring Defendant to delete, destroy, and purge the Private Information of Plaintiffs and Class Members unless Defendant can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;
  - f) Requiring Defendant to implement and maintain a comprehensive security program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Private Information;
  - g) Requiring Defendant to engage independent third-party security auditors and conduct internal security audit and testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;
  - h) Requiring Defendant to engage independent third-party security auditors and/or internal personnel to run automated security monitoring;
  - i) Requiring Defendant to create the appropriate firewalls, and implement the necessary measures to prevent further disclosure and leak of any additional information;

1 j) Requiring Defendant to conduct systematic scanning for  
2 data breach related issues;

3 k) Requiring Defendant to train and test its employees  
4 regarding data breach protocols, archiving protocols, and  
5 conduct any necessary employee background checks to  
6 ensure that only individuals with the appropriate training and  
7 access may be allowed to access the Private Information  
8 data; and

9 l) Requiring all further and just corrective action, consistent  
10 with permissible law and pursuant to only those causes of  
11 action so permitted.

12 4. That the Court award Plaintiffs and the Class damages (both actual  
13 damages for economic and non-economic harm and statutory  
14 damages) in an amount to be determined at trial;

15 5. That the Court issue appropriate equitable and any other relief  
16 (including monetary damages, restitution, and/or disgorgement)  
17 against Defendant to which Plaintiffs and the Class are entitled,  
18 including but not limited to restitution and an Order requiring  
19 Defendant to cooperate and financially support civil and/or criminal  
20 asset recovery efforts;

21 6. That the Court award Plaintiffs and the Class pre- and post-judgment  
22 interest (including pursuant to statutory rates of interest set under State  
23 law);

24 7. That the Court award Plaintiffs and the Class their reasonable  
25 attorneys' fees and costs of suit;

26 8. That the Court award treble and/or punitive damages insofar as they  
27 are allowed by applicable laws; and  
28

9. That the Court award any and all other such relief as the Court may  
deem just and proper under the circumstances.

**VI. JURY TRIAL DEMANDED**

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs respectfully  
demand a trial by jury for all claims.

DATED: July 31, 2025,

CLARKSON LAW FIRM, P.C.

/s/ Yana Hart

Yana Hart

Mark Richards

Bryan Thompson

22525 Pacific Coast Highway

Malibu, CA 90265

Tel: (213) 788-4050

yhart@clarksonlawfirm.com

mrichards@clarksonlawfirm.com

bthompson@clarksonlawfirm.com

CLAYEO C. ARNOLD

A PROFESSIONAL CORPORATION

M. Anderson Berry

Gregory Haroutunian

12100 Wilshire Boulevard, Suite 800

Los Angeles, CA 90025

Tel: (747) 777-7748

Fax: (916) 924-1829

aberry@justice4you.com

gharoutunian@justice4you.com

bjack@justice4you.com

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

John J. Nelson

280 S. Beverly Drive

Beverly Hills, CA 92102

Tel: (858) 209-6941

jnelson@milberg.com

*Interim Co-Lead Counsel for Plaintiffs  
and the Proposed Class*